FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA **17-MJ-524 JWF**

-vs- **GOVERNMENT'S MOTION OPPOSING RELEASE**

WILLIAM R. ROSICA,

Defendant.

The United States of America, by and through its attorneys, James P. Kennedy, Jr., Acting United States Attorney for the Western District of New York, and Craig R. Gestring, Assistant United States Attorney, of counsel, hereby files its response to the motion filed by defendant WILLIAM ROSICA on or about May 25, 2017, seeking *de novo* review of the Magistrate Courts Detention Order issued March 3, 2017. The United States respectfully asks this Court to uphold the Magistrate's findings that no condition or set of conditions would reasonably assure him that the defendant would comply with any release conditions and that there were no condition or set of conditions which would reasonably assure the safety of the victim.

THE FACTS

Between February 2016 and March 2017, defendant WILLIAM ROSICA subjected the victim[1] to a nonstop sadistic campaign of terror and psychological torture intended to kill, injure, harass, and intimidate her. ROSICA used direct, indirect, and digital surveillance in a focused campaign of online abuse, physical stalking, and harassment to destroy all aspects of the victim's life.

[1] The victim will not be identified in this filing, but her identity is known to the government.

Background

In February 2016, the victim ended a three-year relationship with ROSICA. Within a month of their break up, the victim started to receive anonymous harassing text messages, phone calls, and emails. The emails were from multiple generic email addresses including *trustmeiknow@yahoo.com*, *anonymous@textem.net*, and *iamonit@yahoo.com* [2]. These emails and text messages directly referenced her relationship with the defendant and were often obscene. The emails and text messages increased and became more aggressive and hostile around May 2016 when the victim broke off all contact with ROSICA.

While this anonymous harassment was increasing, ROSICA also continued to directly contact the victim via email and text messages from his known email accounts. In many of these communications, ROSICA would make similar comments or refer to similar topics as those in the anonymous harassing emails. He would also comment on the victim's medical history and his belief that she had mental health problems.

The Threat to Destroy the Victim's Life

In late August 2016, the victim agreed to meet ROSICA in person. At that meeting, ROSICA told the victim *"I am at a cross-roads. Either I let you walk away and we live our separate lives or short of killing you, I destroy every aspect of your life. You tell me what I should do."* The victim told ROSICA that she wanted to be left alone and walked away. The victim identified this meeting as another milestone after which the harassing emails and text contacts increased. Approximately one week later, ROSICA sent an email to the victim which

[2] ROSICA used a spoofing website to create and send these emails. Spoofing sites allow a user to send an email or text message, or create a fictitious email account, while concealing the sender's real identity. Evidence of this activity was found on ROSICA'S computers during a forensic examination.

included the following, "…*And with regard to our last conversation in the park, I still remain at a cross-roads. I must protect my better interests*." The victim took both these references as a direct personal threat to harm her.

The AT&T Phone Account Attack

In early September, the victim started receiving multiple automated text messages from AT&T, her cellular phone provider. These messages related to someone resetting her password and attempting to access her online cellular account. Throughout the month of September, additional text messages were received from AT&T showing multiple attempts to access the victim's online cellular account. Around the middle of September, the victim changed cellular phone numbers and her online account ID. However, despite changing her online ID, the victim continued to receive the same AT&T automated text messages with the new online ID showing that someone was still trying to access her cellular account.

The Fictitious Katy Jones Texts/Emails

At around this same time, the victim was contacted by ROSICA who claimed that the same thing was happening to his online cellular account. ROSICA specifically identified the person hacking into his account as "Katy Jones" and claimed that Jones was harassing him via email as well. He claimed that he was working on identifying Jones and was going to file a police report. He claimed that the harassment left him "pissed, exhausted and frustrated." He told the victim that he did not want "anyone knowing my business (which could also drag

you into this)." The investigation recovered emails purportedly sent to ROSICA from *katy.jones76@yandex.com* and *katy.jones76@muchomail.com* [3].

ROSICA continued to use the Katy Jones identity to abuse and harass the victim and her family. On one occasion, the victim's ex-husband received text messages purporting to be from Jones on his own cellphone. These texts were intended to injure, abuse, harass, and intimidate the victim's ex-husband as well as the victim herself. The texts specifically referenced the fact that the victim was recently at the home of her ex-husband, and that Jones would send ROSICA a photo of the victim's car in her ex-husband's driveway; a fact which would only be known through physical surveillance of the victim. The text messages also suggested that the victim's ex-husband was a drunk, and accused him of being physically abusive towards the victim. The text messages also said that Jones would make sure that "Bill" knew what was going on.

Shortly after this exchange, ROSICA forwarded an email message from his known email account to the victim which he claimed he received from Katy Jones. The content of the original forwarded message stated, "this is [victim's] new car parked at her ex-husband's house on [ex-husband address] have her explain why she is at her ex's house when she has made it known he was abusive to her shes even helping him do yard work in her kaki shorts and grey t-shirt this was taken on sunday 9 18 aroun [sic] 1 pm". The victim confirmed receiving a picture in the email that showed her new vehicle in her ex-husband's driveway. A digital copy of the image was provided to the FBI, which showed a Honda CRV with a NY license plate matching that of the victim's vehicle.

[3] The FBI determined that these emails were actually created and sent by ROSICA to himself in furtherance of his cyberstalking activity.

In this same email, ROSICA wrote "When you decided to start sending things back to me with my name on them in July, that's when I suspected you had someone else. We started talking again and I begged for you to tell me the truth and you kept lying, as is evident now. You knew I knew. I felt sorry for you because I thought you were going to kill yourself again like you did several years ago. Remember when you were in-patient psych for downing all of those phenobarbital pills??... Better yet, maybe your son needs to know just how psycho you are… Did you bring Gypsy with you to [victim ex-husband's] today or did you leave her home in the crate again? …Both Doctors were right about you—Borderline Personality Disorder along with Mania and Depression (although you only ever admitted to the depression). You are pathetic, PSYCHO, a LIAR, and the MOST untrustworthy person I have ever met… What would your son think of his mother being suicidal? That is where you are headed. You have created such messes in your life that you will end up having no other option."

The Work Computer Attacks

In addition to the hacks of her personal online accounts and the months of ongoing harassment, the victim's employer's email system was also hacked. In October 2016, the IT Manager for the victim's employer learned that someone attempted to hack her work email account. The IT Manager checked access logs, enabled two-factor authentication, and changed passwords. The IT Manager extracted available logs for the previous 180 days and voluntarily provided those to law enforcement. Updated analysis of attempted access into the victim's email account showed *282 unique unauthorized attempts* beginning September 8, 2016 and ending on February 6, 2017. Review of the logs indicated that the unauthorized access

attempts either failed at an invalid password or stopped after a challenge question. These hacks were traced back to IP Addresses which were operating as Tor Network exit nodes [4].

ROSICA also used multiple fraudulent email accounts to try to get the victim fired from her job. The defendant sent numerous emails over several months to the victim's employer and her direct supervisors which claimed that the victim was: looking for work elsewhere; mentally unstable; unhappy with her salary; having an affair with a co-worker; untrustworthy; and other false allegations designed to harm the victim. The investigation determined that many of these accounts were also created using identifying information which showed they were created from Tor exit nodes.

In January 2017, the FBI obtained a search warrant and Pen Register Trap and Trace Order to identify the user of some of the email accounts used to harass the victim at work. Because the user was hiding behind the anonymity of the Tor network, conventional IP Address information alone could not be used to identify them. However, the FBI was able to identify the actual IP Address of the person associated with these fraudulent accounts to be WILLIAM ROSICA. Further proof was obtained when evidence of a file sent to one of the fraudulent email addresses was forensically recovered from ROSICA'S seized computer during analysis conclusively linking him to the fraudulent and harassing emails.

It should be noted that an executable Tor browser was also recovered from a digital device at the defendant's residence following his arrest.

[4] Use of the Tor network masks the user's actual Internet Protocol ("IP") address, which could otherwise be used to identify a user, by bouncing user communications around a network of relay computers (called "nodes") run by volunteers. To access the Tor network, users must install Tor software either by downloading an add-on to their web browser or the free "Tor browser bundle." When a Tor user visits a website, the IP address visible to that site is that of a Tor "exit node," not the user's actual IP address, Tor is designed to prevent tracing the user's actual IP address back through that Tor exit node. Accordingly, traditional IP-address-based identification techniques used by law enforcement on the open Internet are not viable.

Surveillance Texts and Emails

During this same time, the victim started getting harassing texts and emails from other accounts, including ones that purported to be from a neighbor. These emails and text messages contained information that could only have been obtained through physical surveillance of the victim. These messages included information on where the victim parked her car at night, which lights were left on at the victim's home, and the routes the victim used to travel to and from work.

ROSICA tries to get the victim to commit Suicide.

On or about October 25, 2016, the victim received four separate text messages from anonymous accounts with references to committing suicide. The messages contained links to: "the 7 easiest and best ways to commit suicide"; "the-ten-minute-suicide-guide.html"; "10-simple-ways-to-commit-suicide" and "7- easiest- painless- ways- of- killing- yourselves-quickest." All four messages were sent by ROSICA from fictitious email addresses.

Four days later, the victim again received multiple text messages from anonymous accounts which encouraged the victim to commit suicide. These texts included: 1) *trailer trash lying cheating psycho u ruin everything you touch liar liar psycho liar cheater cheater liar psycho go take some pills lots of them*; 2) *watching the move [sic] "me before you" twice in one week is a good sign your thinking of killing yourself again good for you do it right this time psycho* [5]; 3) *watch more suicide related movies then take some more of your pills*; 4) *SUBJ: 99 Little Known Facts about suicide MSG: watch*

[5] The investigation determined that ROSICA had accessed or tried to access the victims Time Warner Cable account more than 220 times over a three month period of time. During these intrusions, ROSICA would pretend to be the victim while communicating with TWC and he would get information on the victim and her account, to include recent movies watched by the victim. He would then use this unlawfully obtained information in other emails to the victim to show that he knew her every move. ROSICA did the same to other victims, and would routinely reset their cable and phone service to harass, annoy, and cause harm to the victims.

more suicide related movies and tell people you are not psycho and crazy take plenty more pills you are out of your mind and a liar; and 5) *SUBJ:Sent by IP 46.166.188.209 MSG: interesting movie selections more suicide flicks*? A portion of those text messages also provide medical characteristics of individuals with personality disorder (for example, 'people with personality disorder are also usually very impulsive, oftentimes demonstrating self-injurious behaviors'). Based on ROSICA'S prior references to suicide, it is clear that these emails were sent with the intent to kill, injure, harass, or intimidate the victim.

The Medical Record Attacks

In addition to the hacks of the victims cellphone account, personal email account, cable account, and work accounts, ROSICA also attempted to remotely access the victim's medical records through her University of Rochester online patient portal account. Specifically, on November 30, 2016, two attempts were made to remotely access the online University of Rochester MyChart account containing protected medical information for the victim. The attempts were identified via automated Login ID recovery emails sent to victim's personal email account.

Throughout this time, ROSICA also continued to attempt to access protected health information on the victim through her pharmacy. On December 7, 2016, the victim received a phone call from Walgreens stating her prescription was ready for pick-up. After speaking with the pharmacist, the victim stated that she had previously cancelled all her auto-refill prescriptions but for some reason this one was not cancelled. After picking up her prescriptions the evening of December 7, 2016, the victim received an email from weknow@hotdak.net with the message: "bout time you picked up youre psyche pills at drug

store youre driving is not great either hurry home so you can go to trailvervile how does it feel deep in youre mind to know you are a skank liar? …. don't be surprised how many people know all of this… a suicidal skank liar so many people know that now…"

An interview with the victim's pharmacy identified a pattern of anonymous and fake phone calls inquiring about the victim's medications. The employees at the pharmacy documented phone calls on September 26, 2016; October 20, 2016; seven times on December 1, 2016; December 2, 2016; December 3, 2016; December 4, 2016; December 6, 2014; December 14, 2016; December 15, 2016; twice on December 16, 2016; December 29, 2016; four times on December 30, 2016; January 2, 2017; and January 4, 2017.

In addition to these attempts to access the victim's protected pharmacy records, someone called Walgreens impersonating the victim's primary care physician on January 2, 2017. The FBI interviewed the Pharmacist who took that call and confirmed an attempted call from someone who claimed they were with the 'Office of [the victim's doctor]' and wanted to know details of medication for the victim. The caller hung up after the Pharmacist asked for more information regarding the Doctor's office.

The Valentine's Day Attack

On February 14, 2017, Valentine's Day, the victim received a delivery of Roses at her place of employment from FTD. These flowers were addressed to her, and were accompanied by a card which read "*All of us here at the Mental health Clinic want to wish you a Happy Valentine's Day and to congratulate you on your progress.*" Records checks with FTD determined that a person using the victim's name and home address ordered the flowers and paid for them with

a pre-paid credit card[6]. FTD data records show that the purchase was made from a Tor exit node on February 10. During this time, the FBI was operating a Court authorized Pen Register Trap and Trace device on ROSICA'S home internet connection. That Trap and Trace confirmed that at the same time the FTD order was placed online from a Tor exit node, ROSICA was operating a Tor session from his home.

Agents were able to obtain the full pre-paid credit card number associated with the FTD Purchase. Records from the company that issued the card showed that the same card was sold on February 10, a few hours before the FTD Order was placed. The card was sold from a WalMart located at 1490 Hudson Ave, Rochester, New York, which is the closest WalMart location to ROSICA'S home and work addresses. Agents visited the store and were able to obtain records related to the purchase of the pre-paid credit card. They also obtained and reviewed store surveillance video of the purchase transaction. These videos clearly show the defendant, WILLIAM ROSICA purchasing the pre-paid credit card and leaving the store with it, before getting into his pickup truck and driving away.

The Physical Stalking

In addition to his relentless digital stalking, ROSICA also physically stalked the victim in the real world. The investigation determined that ROSICA would conduct surveillance of the victim when she was at home, at work, or when she was out. He would also follow her when she was running errands or visiting others, including friends or family members.

[6] Pre-paid credit cards are obtained using cash, and can be used like any other credit card, including online. However, since they are generic, no bank information, card holder's name, or identifying information is recorded during the purchase.

ROSICA would then capitalize on this surveillance data through emails to the victim showing her that he knew where she was at all times.

Text and email messages from the non-existent Katy Jones contained close-up photos of the victim's car, photos of the victim's car in her ex-husband's driveway, and photos of ROSICA'S home, taken on various dates and times. On one occasion, ROSICA claimed that Jones had taken a photo of the victim's car (which was cropped to show only the rear of her car including her license plate) and then sent it to him. He sent the photo to the victim from his own email account to prove that he too was being "stalked." However, forensic review of ROSICA'S computer found the full, uncropped photo of the victim's car, which was taken at the victim's place of employment, *on his computer*. This photo contained digital metadata showing that the photo was physically present on ROSICA'S computer *before* the email supposedly containing the photo was ever sent to him by Jones. Several other photos, allegedly sent to ROSICA by Jones, were also found on his computer with metadata showing that their physical presence on his computer predated the emails from Jones which allegedly contained the same photos [7]. This evidence proves that ROSICA and Jones were in fact one and the same person.

ROSICA would drive by the victim's home at all hours of the day and night in order to harass the victim. A pole camera set up by law enforcement during the latter part of the investigation captured ROSICA driving by the victim's home on multiple occasions. Significantly, ROSICA did not only conduct surveillance in his own vehicle, a distinctive pickup truck, known to the victim. The investigation uncovered the fact that ROSICA would

[7] Many of the surveillance photos allegedly taken and sent by Jones were sent in a cropped, or edited version. However, examination of the full uncropped photos physically recovered from ROSICA'S computers showed the side view mirror of the vehicle from which the photos were taken. Analysis of these images showed that these photos were actually taken from ROSICA'S distinctive pickup truck.

often borrow vehicles from friends and co-workers for short periods of time. When questioned, ROSICA would either lie about why he was borrowing their cars, or say he was using their vehicles to check up on his girlfriend. ROSICA would also rent vehicles from several places, including an Enterprise Rental location near the victim's home.

During these rental periods, ROSICA would frequently return to the rental counter and switch cars, claiming that he was doing "PI" work. He often requested cars with tinted windows. On at least one occasion, rental records show ROSICA renting a distinctive vehicle from Enterprise only to have that same distinctive vehicle appear on and be captured by the pole camera near the victim's home shortly thereafter; thus proving that ROSICA was physically stalking the victim and also that he was attempting to mask his crimes by changing vehicles.

Physical Stalking by Proxy

In addition to conducting surveillance himself, ROSICA directed other third parties to drive by the victim's home and report their observations back to him. ROSICA would then use this information to further terrorize the victim into believing that he was always watching her. Some of the people ROSICA directed knew that he was gathering intelligence on his girlfriend and willingly participated [8,9]. However, others, including other police officers, were

[8] ROSICA directed one confederate to purchase "burner phones" and prepaid phone cards from the WalMart located on Hudson Avenue in Rochester (the same WalMart where ROSICA purchased the pre-paid credit card he used to send the flowers to the victim on Valentine's Day). ROSICA would pay that person in cash and directed that person to throw away the wrapping material of the new phones before giving them to him. ROSICA also requested that same individual go out to the victim's home, and switch out the victim's trash with a bag that ROSICA would give him.

[9] ROSICA directed another confederate to conduct physical surveillance on the victim for him on more than a dozen occasions. ROSICA also requested that this individual pull the victim's trash for him.

not told the true purpose for his request. ROSICA used his official position with the Irondequoit Police Department to get Police Officers in the victim's hometown to drive by her home and report her status to him "off the record." He made this same request to at least three Police Officers on various shifts, changing his story as to why he needed the information with each one. To their credit, none of the Police Officers he approached did so. In fact, they reported his suspicious requests to their Patrol Sergeant who confronted ROSICA by phone and told him to have no further contact with these officers. ROSICA responded to this conversation with "are we on a recorded line."

The investigation did uncover that ROSICA had approached other Police Officers, including some in his own department, and had them run license plates or perform other official actions in support of his unlawful surveillance activities. However, these officers were not told the true reason for ROSICA'S requests and believed that they were performing authorized law enforcement work. Official records do show that ROSICA himself ran the victim's license plate multiple times using his official access to law enforcement databases as a Police Officer. The investigation also determined that ROSICA ran other personal license plates using his official access to law enforcement databases to include at least one former girlfriend[10].

Threats made by ROSICA

In addition to the threats made to the victim discussed above, the facts show that ROSICA also made threats to harm others during the same time he was terrorizing the

[10] Records show that ROSICA even ran a former girlfriends license plate after she had already surrendered the plate making it unlikely that the request was official in nature.

victim[11]. These threats were made while the defendant was on and off duty as a Police Officer. Federal investigators recovered an application from ROSICA'S cellular phone which he used to record many of the phone calls he made. However, the app continued to record ambient conversations using the phones microphone even after ROSICA disconnected the phone calls. This produced a large collection of digital recordings in which ROSICA effectively recorded himself having conversations with other people.

In one of these recordings, dated February 27, 2017, only a week before his arrest, ROSICA is recorded speaking with his son about his estranged wife's medical diagnosis. During that call ROSICA threatens to physically harm her doctor. Specifically, ROSICA says;

> *If a doctor is offended by a second opinion, then fuck him, I'll beat his ass, alright, or I'll let you do it…I'll sit back and watch.*

ROSICA then talks about coming to the hospital early the next day and says:

> *I'll bring my gun, I'll bring my gat with me, I'll bring my heater. Listen Doc, See this right here, I got some…I got a second opinion for you….I got me a .380, I got me a .40, I got me a couple of .45's, take your pick [12]. (laughing).*

ROSICA also records himself making threats involving civilians while on duty as a Police Officer. In one file, dated December 31, 2016, ROSICA records himself while at work. During this recording, which lasts about an hour, ROSICA is investigating a report of a teenager who left home. The recording captures ambient sounds to include conversations with

[11] In his motion for reconsideration of the Magistrate's Detention Order, the defense argues that ROSICA does not pose a threat of physical or bodily harm. However, the facts set forth in this filing demonstrate that ROSICA has and continues to pose a threat of physical or bodily harm.

[12] .380, .40, and .45 are all firearm calibers. Significantly, at the time of his arrest, ROSICA possessed a .380 caliber pistol, a .40 caliber pistol, and two .45 caliber pistols (one of which was his issued duty pistol) – consistent with the pistols mentioned in his threat.

witnesses, the police vehicle's engine racing, and police dispatch audio in the background. ROSICA makes and receives several phone calls throughout the recording, and identifies himself several times as "Officer Rosica." At one point, ROSICA is talking with someone in his patrol car about the missing child's grandmother, who he believes spoke to him disrespectfully. The recording captures ROSICA saying in an aggressive and hostile tone;

> *That fucking nigger, girlfriend's nigger grandmother, was saying I ain't gotta tell you nothing....Fuck her that fucking nigger, Fucking nigger, I'll go over there and fucking punch her nigger fucking mouth.*

Later in that same recording, ROSICA is again in his patrol car speaking with an unidentified female[13] about the missing teenager and records himself saying:

> *What a fucking little fucking bastard. Un-fucking believable...fuck do you think you are?...I want to get him alone, I want to get him alone before I get him with his parents. Have a fucking little wall to wall counseling session [14] with his little nigger ass.*

ROSICA eventually locates the child and confronts him in a loud and aggressive manner. During these recordings, ROSICA becomes more and more enraged. He is recorded raising his voice to civilians, cursing at people in traffic, and using racial epithets. ROSICA also threatens to physically assault people on more than one occasion. The Court should consider the fact that ROSICA made these threats to harm others during the same time period that he was physically and digitally threatening the federal victim's life, and while he was working – on duty – as a Police Officer.

[13] The recordings indicate that the female was in the patrol car with ROSICA at the time. The recording also suggest that she is a civilian.

[14] The term "wall to wall counseling" is military jargon for a behavior correction method in which a superior shows a subordinate the error of his or her actions by means of physical violence. Applications of wall-to-wall counseling vary, ranging from a simple slap to prolonged sessions ending with a trip to the hospital. This definition is taken from an open source internet search. ROSICA previously served in the US Army.

Obstruction of Justice

The facts definitively show that ROSICA obstructed the investigation of his crimes before and after his arrest. As previously noted, ROSICA made extensive use of the Tor network to stalk his victims specifically because of the anonymity that Tor provides. ROSICA went to great lengths to conceal his identity while engaging in a sophisticated scheme to terrorize this victim for almost a full year. ROSICA created fraudulent email accounts. ROSICA used spoofing software to misdirect the investigation. ROSICA even created a fictitious antagonist, *Katy Jones*, who he could blame if he ever got caught. But that was not enough. ROSICA had anti-forensic software and wiping tools on his computer which are designed to remove or destroy digital evidence. ROSICA also used standard law enforcement countermeasures to avoid detection to include; changing phones, changing vehicles, and changing fraudulent email accounts. In short, he did everything he could to obstruct the investigation of his crimes, including misusing his law enforcement training and resources.

But his pattern of obstruction did not end with his arrest. ROSICA continued to manipulate and lie to federal agents throughout his post arrest interview in March 2017. At the time of his arrest, ROSICA was in his Police uniform on the way to work. The video of his interview shows that from the very beginning, ROSICA used his position to attempt to "bond" with the agents conducting his interview. He kept throwing out references to cases they worked together, and names of other members of the Rochester law enforcement community they knew in common. He also continued to use his position as a Police Officer to try to manipulate the agents and influence the direction of their investigation.

But most significantly, ROSICA lied to federal agents during his interview[15]. When agents asked him when he last saw the victim, ROSICA lied. When agents asked if he used Tor, again ROSICA lied[16]. Astonishingly, ROSICA blamed Katy Jones for the emails and text messages. He told the FBI that she was actually to blame for the whole situation, going so far as to suggest that *the victim was actually Jones,* and that Agents should investigate this connection. This was not just another lie, this was part of ROSICA'S plan all along – and the reason he created Katy Jones in the first place. As previously noted, *ROSICA actually was Katy Jones*, so his suggestion that Agents investigate the victim for being Katy Jones was a deliberate and material false statement aimed at obstructing and misdirecting the federal criminal investigation.

ROSICA was detained at his initial appearance, and again, following a full detention hearing held on March 3. He has remained in custody since then. A motion for reconsideration of the Magistrate's Detention Order was filed by Counsel on May 25, 2017. The United States respectfully asks this Court to uphold the Magistrate's Detention Order.

THE DEFENDANT SHOULD BE DETAINED

Title 18, U.S.C., § 3142(e) mandates that a judicial officer order the defendant detained if no conditions will reasonably assure his/her appearance; the safety of the community; or to prevent the serious risk that the defendant will obstruct or attempt to obstruct justice, or

[15] ROSICA'S false statements to federal agents constitute yet another felony (violation of Title 18, United States Code, Section 1001) committed while he was a sworn law enforcement officer.

[16] ROSICA denied using TOR during his interview with the FBI, however, the investigation showed that ROSICA had in fact used TOR less than 6 hours before he was arrested.

that he will threaten, injure or intimidate a witness or attempt to do so [17]. Before making such a finding, a court must consider all reasonable less restrictive alternatives to detention. *United States v. Song*, 934 F.2d 103, 105 (7th Cir. 1991). However, the Bail Reform Act of 1984 does not require release of a dangerous defendant if the only combination of conditions that would reasonably assure societal safety consists of heroic measures beyond those which can fairly be said to have been within Congress's contemplation. *United States v. Tortora*, 922 F.2d 880, 887 (1st Cir. 1990).

After a motion for detention has been filed, the Court must undertake a two-step inquiry. *United States v. Fredmond*, 837 F.2d 48, 49 (2d Cir. 1988), citing *United States v. Shakur*, 817 F.2d 189 (2d Cir. 1987). It must first determine by a preponderance of the evidence that the defendant presents a risk of flight or by clear and convincing evidence that the defendant poses a danger to any other person and the community, or that he poses a serious risk that the defendant will obstruct or attempt to obstruct justice, or that he will threaten, injure or intimidate a witness or attempt to do so. See *United States v. Jackson*, 823 F.2d 4, 5 (2d Cir. 1987), *Fredmond*, *Id*. Upon making this determination, the court then turns to whether any condition or combination of conditions of release will protect the safety of the community and reasonably assure the defendant's appearance at trial. *Id*.

Title 18, U.S.C., § 3145(a)(1) allows a party to file with the District Court a motion for review of a release order issued by a Magistrate. The District Court reviews the Magistrate's detention decision de novo. *United States v. Leon*, 766 F.2d 77, 80 (2d Cir. 1985). In making

[17] The government incorporates all previous argument made on March 3, 2017, as well as the facts set forth in the criminal complaint in this response.

its findings, the District Court need not defer to the Magistrate Judges' findings or give specific reasons for rejecting them.

The District Court may rely on the transcript of proceedings below, take additional evidence in conjunction with the transcript or conduct a full de novo evidentiary hearing. See e.g. *United States v. Koenig*, 912 F.2d 1190, 1193 (9th Cir. 1990); *United States v. Delker*, 757 F.2d 1390, 1393-94 (3d Cir. 1985); *United States v. Fortna*, 769 F.2d 243, 250 (5th Cir. 1985); *United States v. Maull*, 773 F.2d 1479, 1481-1482 (8th Cir. 1985) (en banc).

When deciding whether there are conditions of release that will reasonably assure the appearance of the person as required and the safety of any other person and the community, courts are instructed to take into account the available information concerning those factors enumerated at Section 3142(g). These factors include: (1) the nature and circumstances of the offense charged, including whether the offense is a crime of violence or involves a narcotic drug; (2) the weight of the evidence against the person; (3) the history and characteristics of the person, including (A) the person's character, physical and mental condition, family ties, employment, financial resources, length of residence in the community, community ties, past conduct, history relating to drug or alcohol abuse, criminal history, and record concerning appearance at court proceedings; and (B) whether, at the time of the current offense or arrest, the person was on probation, on parole, or on other release pending trial, sentencing, appeal, or completion of sentence for an offense under federal, state, or local law; and (4) the nature and seriousness of the danger to any person or the community that would be posed by the person's release. *Id*.

The Magistrate carefully reviewed and considered the facts and the evidence adduced at the detention hearing before determining that no condition or set of conditions would

reasonably assure him that the defendant would comply with any release conditions and that there were no condition or set of conditions which would reasonably assure the safety of the victim. In making this determination, the Magistrate considered not just the strength of the government's case, as the defense alleges, but all of the Section 3142(g) factors as is reflected in the transcript of the detention hearing proceeding held on March 3, 2017.

In requesting reconsideration of the Magistrate's Detention Order the defendant's motion does not raise any new facts or information that were unknown to the Court at the time ROSICA was Ordered detained. The defendant's filing mentions ROSICA'S age. The Magistrate already knew the defendant's age. The defendant's filing mentions ROSICA'S ties to the community. The Magistrate already knew how long the defendant lived in the area. The defendant's filing mentions ROSICA'S marital and family status. The Magistrate already knew about the defendant's estranged wife and child.

The defendant's filing mentions ROSICA'S medical and mental health history. The Magistrate already knew about the defendant's cardiac, diabetic, and mental health issues. The defendant's filing mentions ROSICA'S lack of criminal history. The Magistrate already knew that the defendant had no criminal record. Again, none of this information was new to the Court. It either came out through Counsel at the detention hearing or was included in the pre-trial services report - which also recommended detention.

In short, the defendant's filing does not offer any additional facts, evidence, or law that were previously unknown to the Magistrate which would support reconsideration of the Detention Order.

The defendant's filing specifically mentions ROSICA'S employment as a basis for release, suggesting by inference that his work as a Police Officer should mitigate his present

circumstances. However, the facts show that just the opposite is true. First, the Magistrate already knew that the defendant was an Irondequoit Police Officer. In fact, the record shows that ROSICA'S employment was a key factor in determining that there was *a heightened risk* to the victim;

> The Court: Now, again, you're presumed innocent, but as a law enforcement officer there can be no doubt that if you did these things, you knew at the time you were doing them that they could lead to the moment we're both presented with right now where you were apprehended. And despite that risk to yourself, to your family, your job, you were willing to take that risk, according to the Government, and that really concerns me in terms of what you're capable of risking if I was to set conditions of release.
>
> (see *Detention Hearing Transcript*, March 3, 2017, Page 29, Lines 14-23)

Second, the facts show that ROSICA committed a federal felony while wearing a Police Badge and uniform; in fact, he committed multiple federal crimes while so employed. ROSICA took an oath to uphold the law as a Police Officer – an oath that he violated virtually every day that he tormented and terrorized his victims. The fact that the defendant freely and frequently violated that oath suggests that there are no condition or set of conditions which would suddenly now compel him to obey.

Further, ROSICA'S own words, including those recorded while he was on duty as a Police Officer, show his aggressive and violent personality. ROSICA'S comments about a runaway child and that child's grandmother, show a level of vitriol and aggression that are inappropriate in any member of society, let alone one who carries a gun and is charged with being a law enforcement officer. The fact that ROSICA felt safe enough to make those violent statements and threats as a Police Officer then, strongly favor his detention as a danger now.

The United States submits that a review of the 3142(g) factors in this case show by overwhelming evidence, well beyond the clear and convincing standard required, that

ROSICA has already obstructed and attempted to obstruct justice; has already threatened and intimidated a witness; and continues to poses a serious risk that he will obstruct or attempt to obstruct justice, and that he will continue to threaten, injure or intimidate a witness or attempt to do so if released.

There is therefore no legal or factual basis to revoke or amend the Detention Order issued by Magistrate Feldman on March 3, 2017.

CONCLUSION

For the reasons specified herein, the defendant's motion to Revoke or Amend the Detention Order should be denied.

Dated: Rochester, New York
June 20, 2017

JAMES P. KENNEDY, Jr.
Acting United States Attorney

By: /s/CRAIG R. GESTRING
Assistant United States Attorney
Western District of New York
U.S. Attorney's Office
500 Federal Building
Rochester, NY 14614
(585) 399-3900
craig.gestring@usdoj.gov